

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA

IN THE MATTER OF THE SEARCH OF
EMAIL ACCOUNT BELONGING TO
SETH MAJOR:
josephcrocker71@hotmail.com

Case No. 8:24cr829

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT**

I, JOSEPH J. LEA, being duly sworn, declare and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for the email account of Seth Major, josephcrocker71@hotmail.com. (SUBJECT ACCOUNT) which was used during the commission of this fraud scheme. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation USA. (hereinafter Microsoft), an internet service provider headquartered at 1Microsoft Way, Redmond, Washington 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent (SA) of the United States Secret Service (USSS). I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure

41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

3. I am a Special Agent (“SA”) with United States Secret Service (“USSS”) and have been so employed since August 2009. I am currently assigned to the Greenville Residence Office and primarily investigate financial crimes to include wire fraud, identity theft, credit card fraud, bank fraud and money laundering. Prior to becoming an SA with USSS, I was employed as police officer and detective since 2004, where I conducted numerous investigations of fraud schemes. I have received both formal and informal training from USSS and other institutions regarding cyber and financial related investigations, embezzlement, and fraud.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1349 (conspiracy to commit wire fraud); 18 U.S.C. § 1341 (Mail Fraud); have been committed, are being committed, and will continue to be committed by Seth MAJOR.

6. There is also probable cause to search the property described in Attachment A for evidence of these crimes further described in Attachment B.

II. JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

III. PROBABLE CAUSE

A. Background of Investigation

8. The United States Secret Service (USSS), and Anderson County Sheriff's Office (ACSO), Anderson City Police Department, Easley Police Department, and Greenville City Police Department are investigating Seth MAJOR and various other individuals in an ongoing wire fraud scheme. On June 4th, 2024 the Greenville Resident Office was contacted by Harbor Freight corporate security in reference to an excess of half a million dollars of fraud being perpetrated against their company that appears to originate in Anderson, SC. They identified several unknown individuals at the time as obtaining Harbor Freight gift cards and using an unknown exploit to change the value of these cards through the online website and have the items shipped to a residence.

9. Of these items purchased through this wire fraud scheme, many of the items were ultimately returned to the store branches in Anderson, Easley, and Greenville. Often the refund would be issued to the present party's debit or credit card. Along with the items shipped to local residences, there are numerous occasions in which the items are shipped to residences throughout the United States. Those items were typically single item orders and of a higher value. It is unknown if those items were eventually returned to Harbor Freight for a refund. On at least one occasion, more gift cards were acquired with the funds from the return. Harbor Freight provided Agents with the Secret Service some surveillance video of these returns in hopes to identify the perpetrators.

10. Within a few days of reviewing the data provided by Harbor Freight about the purchases, shipments, and refunds, a clear originating pattern began to appear. The activity began sometime around April of 2023 and continued through the initiation of this case. Though the activity spread throughout the nation, the compromised account activity seemed to originate and continue to be linked to the Anderson SC area.

11. The initial start of the activity originated to a group of gift cards being purchased online and orders being quickly made shortly thereafter. Each of the subsequent orders being placed off that first batch of gift cards all were completed from internet protocol (IP) address 97.89.160.62. Using commercial tools, this IP address comes back to Charter Communications in the Anderson, South Carolina area. One of the initial orders placed one this first batch of compromised cards, had a shipment of many items sent to an address near Anderson, 251 Long View Dr, Williamston, South Carolina. A cross check of this address, along with other local shipment locations provided by Harbor Freight, I was able to identify one of the individuals in the surveillance video as Jamie Major, the father of Seth MAJOR who currently lives at 251 Long View Dr. Williamston, South Carolina.

12. Investigation further revealed that other shipments conducted through the use of this fraud scheme were sent to residences of MAJOR's associates such as his father's and sister's residences. In each of these shipments, the name and contact information appear to be made up at random to conceal the recipient of the merchandise. For example, each of the shipments going to Seth MAJOR's home would be shipped in the name Tyler Grayson or some other variant of that name, thus indicating the forethought of the fraudulent nature of the activity.

13. One of the shipments early in the scheme went to 525 Twin Lake Rd. in Greenville, South Carolina in the name Austin Motes. Agents were able to make contact with Motes and ask

about the shipment he received. He stated that he was contacted via FaceBook Marketplace about a transmission he had for sale. The prospective buyer could not afford the item, but offered to trade for the items with some brand new tools. Motes agreed and several items were shipped from Harbor Freight direct to his home, followed by the buyer coming to his home to pick up the transmission. A later photographic lineup was provided to Motes, in which he immediately picked Seth MAJOR out of that lineup.

14. On 6/21/24, Agents made contact with Seth MAJOR at his home at 251 Long View Dr. Williamston, South Carolina. MAJOR allowed agents inside to speak with him in regards to the shipments being sent from Harbor Freight to his home. It was immediately observed that several of the items in question were observable out in the open, new in box, in MAJOR's living room. MAJOR stated that he had been purchasing gift cards from someone online, but could not elaborate further, when pressed about his further knowledge, MAJOR requested an attorney. A business card was given to MAJOR and advised that he does retain that attorney, and the agents left the residence.

15. Agents then made contact with Jamie Major at his residence at 104 Brookforest Dr. Belton, South Carolina. Upon speaking with him, he stated that he has done returns of items to Harbor Freight. He stated that they would arrive via shipment to his home and he would return them to the store and receive credit to his bank card. He also confirmed that he would acquire further gift cards as well. When asked what he does with the returned money and gift cards, he stated that he give them to his son Seth MAJOR as he was instructed by him. Jamie Major also stated that the coordination of this activity occurred over the phone and via text message with Seth MAJOR.

16. Based on the evidence at hand, The local detectives were able to obtain and execute a search warrant of MAJOR at 251 Long View Dr. Williamston, South Carolina. During the execution of that search warrant, numerous items identified as Harbor Freight merchandise was recovered. Many used and un-used gift cards were located, including those matching ones that were obtained by Jamie Major on surveillance video. Several electronic devices were also recovered during that search warrant and it is believed that they could have been used in the orchestration of this fraud scheme.

17. Believing online sales could be the reasoning for the large one time purchased items to be shipping throughout the US, a request was made to eBay for account information related to Seth MAJOR. Those records were eventually returned and positively identified that the items posted for sale on eBay match those eventually purchased from Harbor Freight and sent to random addresses throughout the US. In posting those items for sale, eBay logs the IP address of the account holder at the time of posting. The account held by Seth MAJOR was accessed by the same IP addresses already identified by the fraudulent purchases at Harbor Freight. It appears that Seth MAJOR would post for an example a: PREDATOR 3500 Watt SUPER QUIET Inverter Generator on eBay for \$849.99 on June 14, 2023 from IP address 71.12.71.54. The item was sold on July 13th to an individual in Tennessee. On that same day a purchase was made on Harbor Freight for that same item and shipped to Tennessee. This purchase from Harbor Freight would be for \$899.99 plus applicable taxes. The IP address on the listing for that item on eBay matches the same IP as the previous purchases from Harbor Freight. There are a total of at least 45 items posted and sold in this manner, all seeming to match the items then purchased on Harbor Freight and shipped directly to the eBay Buyer. This activity would account for the later purchases being sent throughout the United States to seemingly unrelated individuals. The purchase of the items Harbor

Freight for more than the listed price on eBay indicates a knowingly operated fraud scheme, as it would serve no legitimate purpose to lose money in this manner.

18. It should also be noted that the posting and sales of these items also identified and corresponded with IP addresses that were masked in what appears to be an attempt to conceal the nature of the activity. The eBay account was also held in Seth MAJOR's name and other identifying information, but under the email address josephcrocker71@hotmail.com. This email also appears in the Harbor Freight illicit purchases in either the standard form or through an iteration such as crockjosephebay2023@gmail.com, c.rockjoeebay2011@gmail.com, which further identifies other previously unknown IP addresses as being likely associated with MAJOR.

19. During the course of the investigation, the account josephcrocker71@hotmail.com (SUBJECT ACCOUNT) was identified on numerous occasions as playing a significant role in the execution of the fraud scheme. Several of the online orders placed with Harbor Freight provided user information. This is the information entered to provide a reliable shipping address as well as name, phone number, and email in which to provide a receipt. On more than one occasion, the email josephcrocker71@hotmail.com was provided. That email was also listed with eBay as the account email for Seth MAJOR, in which it has been confirmed that items posted and sold on eBay were then purchased with the fraudulent gift cards and shipped to the customer. This indicates that correspondence regarding the posting, sale, and shipment of the items he had for sale would be confirmed via an email sent to the SUBJECT ACCOUNT.

20. In my training and experience, I have learned that Microsoft is an internet service provider that provides email access to the general public, and that stored electronic communications, including text, and multimedia messages (photos, audio, or video) for Hotmail subscribers may be located on the computers of Microsoft. Further, I am aware that computers

located at Microsoft contain information and other stored electronic communications belonging to unrelated third parties.

21. If requested, Microsoft maintains in an electronic communications system (18 U.S.C. § 2510(14)) the contents (18 U.S.C. § 2510(8)) of certain electronic communications (18 U.S.C. § 2510(12)) associated with email service providers. *See* 18 U.S.C. §2703(f).

22. Internet Service Providers (ISPs) typically retain certain transactional information about the use of each telephone or device used to access the account on their systems. This information can include log files and messaging logs showing all activity on the account, such as Internet Protocol (IP) address. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular device was involved.

23. ISPs also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, ISPs typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

24. In some cases, subscribers may communicate directly with an ISP about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. ISPs typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

25. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular email account that is retained by an ISP can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled an email account at a relevant time. Further, such stored electronic data can show how and when the account was accessed or used. Such "timeline" information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. Last, stored electronic data may provide relevant insight into the state of mind of the email account's owner and/or user as it relates to the offense under investigation. For example, information relating to the email account in possession of the ISP may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

IV. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

V. CONCLUSION

27. Based on the forgoing, I request that the Court issue the proposed search warrant.

28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

29. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

By this Affidavit, I request that the Court issue a warrant authorizing a search of the Subject Devices (Attachment A) for the information and materials described in Attachment B.

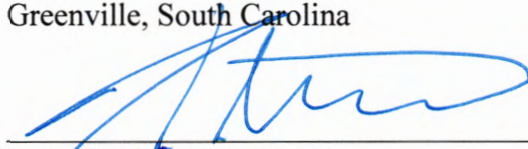
This affidavit has been reviewed by Assistant U.S. Attorney Carrie Fisher Sherard.

Respectfully submitted,



Joseph Lea
Special Agent
USSS

Sworn to me and signed by me
this 17 day of July, 2024
Greenville, South Carolina



KEVIN F. MCDONALD
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the email address JOSEPHCROCKER71@HOTMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation USA. (hereinafter Microsoft), an internet service provider headquartered at 1Microsoft Way, Redmond, Washington 98052

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corporation USA.

To the extent that the information described in Attachment A is within the possession, custody, or control of **Microsoft Corporation USA**., regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **Microsoft Corporation USA**. or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **Microsoft Corporation USA** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. Account Information

- a. User name, primary e-mail address, secondary e-mail addresses, connected applications and sites, and account activity, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;

2. Phone Information

- a. Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device;

3. Evidence of user attribution

- a. Accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).

4. Calendar

- a. All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees;

5. **Contacts**

- a. All contacts stored by **Microsoft Corporation USA**, including name, all contact phone numbers, e-mails, social network links, and images;

6. **Documents**

- a. All user created documents stored by **Microsoft Corporation USA**;

7. **E-mail**

- a. All e-mail messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and e-mails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;

8. **Photos**

- a. All images, graphic files, video files, and other media files stored in the Google Photos service;

9. **Location History**

- a. All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings;

10. **Search History**

- a. All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;

11. **Voice**

- a. All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voice-mail messages sent by or from the Google Voice account associated with the target account/device;

12. Android Auto

- a. All information related to Android Auto including device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs, text messages (SMS), voice actions, and all location.

13. Time Period

- a. All records shall be for the time period of **November 1, 2022 through the current date.**

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1343, 1349 involving Seth MAJOR, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The receipt, distribution, of illicit products, co-conspirators, storage facilities for financial products, record, and proceeds;
- b. Evidence indicating how and when the email service and associated internet services was used to determine the chronological context of email use, account access, and events relating to the crime under investigation;
- c. Evidence indicating the geographic location of the cellular device used to connect to the online email service at times relevant to the investigation;
- d. Evidence indicating the email's owner or user's state of mind as it relates to the crime under investigation;

e. The identity of the person(s) who created the account associated with the email account and/or used the email account, including records that help reveal the whereabouts of such person(s).

f. The identity of the person(s) who sent to and/or received communications from the account about matters relating to obtaining of illicit products, including records that help reveal their whereabouts.